面向企业私有云的数据安全保护方法研究 *

陈 庄，齐 锋

(重庆理工大学 计算机科学与工程学院，重庆 400054)

摘 要：针对现有企业私有云面临的数据安全存储和完整性校验问题，提出一种新的数据线性加扰混合加密保护方法。首先在数据加密之前进行数据细粒度和线性分割线划分；其次，分别对分割后的子数据块进行数据加扰处理；最后使用国产密码算法对加扰数据块进行混合加密和完整性校验。将所提出的算法与 SM4 和 SM2 加密算法进行比较，并通过实验分别对算法的正确性、加密文件类型、加解密效率和安全性进行评估。实验结果表明，相对于另外两种加密算法，提出的算法在兼顾加解密效率的同时安全性得到大幅度提升。

关键词：私有云；国产密码算法；数据线性加扰混合加密；数据完整性

中图分类号：TP309.2 doi: 10.19734/j.issn.1001-3695.2018.08.0652

Research on data security protection method for enterprise private cloud

Chen Zhuang, Qi Feng

(*College of Computer Science & Engineering, Chongqing University of Technology, Chongqing* 400054, *China*)

Abstract: The existing enterprise private cloud is facing a problem about data security storage and integrity verification, this paper proposed a new data linear scrambling hybrid encryption protection method. Firstly, the data are fine-grained and linearly divided before they encrypted. Secondly, the divided sub-blocks are respectively subjected to data scrambling processing. Finally, the domestic cipher algorithm is used to perform mixed encryption and integrity check on the scrambled data blocks. The proposed algorithm is compared with the SM4 and SM2 encryption algorithms, and through experiments evaluate the correctness, encryption file type, encryption and decryption efficiency and security of the algorithm. The experimental results show that compared with the other two encryption algorithms, the proposed algorithm can greatly improve the security while improving the encryption and decryption efficiency.

Key words: private cloud; domestic cryptographic algorithm; data liner scrambling hybrid encryption; data integrity

chinaXiv:201901.00027v1

0 引言

近年来云计算技术行业快速发展，逐渐替代传统 IT 行业，被看做是第三次 IT 浪潮。云计算技术在物联网、移动计算、大数据等行业具有广阔的应用前景，它具有按需扩展、存储整合、经济高效等优点，受到广大企业用户的青睐。云计算[1]在全球范围内目前尚未有统一的标准分类，根据目前业界达成的基本共识，按照服务类型可以分为基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS），按照运营模式可以分为公有云、私有云和混合云。

云计算技术在迅猛发展的同时数据安全问题也日益突出，安全事件不断发生。例如，2016 年 9 月，雅虎在谈判中向 Verizon 推销他们时宣布，至少有 5 亿的用户名、密码、电话号码等信息被泄露；2017 年 6 月，营销公司 Deep Root Analytics 托管在 AWS S3 上的数据库泄露，近 2 亿美国人的投票数据被暴露；2017 年 11 月，有媒体发布消息称趣店百万学生的数据疑是外泄。基于以上原因，目前越来越多的企业用户选择私有云架设方案来应对数据安全问题，其主要原因是企业用户可以拥有数据的控制权限，同时它可以部署在企业数据中心的防火墙内部。防火墙可以有效阻断物理层到应用层之间的攻击行为，但是无法应对在业务逻辑层或数据层的 SQL 注入、数据爬虫、业务权限滥用等非法入侵行为，不能从根本上防止数据泄露问题。

为确保企业私有云环境下的数据安全，本文提出了一种新的不完全依赖密钥的数据安全保护方法即数据线性加扰混合加密算法 DLSHE（data liner scrambling hybrid encryption）。

1 相关工作

私有云相对于公有云和混合云而言，具有更高的安全性，用户不会失去对数据的管控权限，但是同样面临着企业核心数据泄露问题，只是极大的缩小了信息泄露的范围。从目前的研究成果来看，学术界和商业界主要关注点在云数据的安全存储和安全审计两个方面。

在加密存储技术方面，目前绝大多数云供商提供的加密存储服务都是基于美国开发的密码技术标准。现代密码技术按照密钥类型的不同通常可以分为两大类：对称加密算法和非对称加密算法。对称加密算法指的是加密密钥与解密密钥相同的算法，具有加解密效率高的优点，常见的对称加密算法有 AES、DES、3DES 等[2~4]；非对称加密算法指的是加密密钥与解密密钥不同的算法，具有安全性高的优点，常见的非对称加密算法有 RSA、ECC 等[5,6]。同时学术界在同态加密技术、基于属性的加密技术等方面也有大量的研究，但是由于各种原因导致其无法进行大规模的商业应用[7]。

安全审计技术，主要面临着数据持有问题和数据完整性问题。公有云和混合云条件下，主要针对不可信或半可信的云存储系统，文献[8]提出对可证动态数据持有机制进行研

收稿日期：2018-08-21；**修回日期：**2018-10-07 **基金项目：**重庆市研究生科研创新基金资助项目（CYS18312）

作者简介：陈庄（1964-），男，重庆人，教授，博士，主要研究方向为密码学、网络与信息安全研究（cz@cqut.cn）；齐锋（1991-），男，河南信阳人，硕士研究生，主要研究方向为信息安全、应用密码学.

ChinaXiv合作期刊

chinaXiv:201901.00027v1

究，它支持所有的动态操作，但是该方案的执行效率不高；在文献[9]中 Wang 等人提出了一种云存储完整性审计机制，但是计算代价巨大;在文献[10]中徐剑等人提出一种外包数据认证模型，通过外包数据服务器返回的证据和先前计算的正确性根据进行对比就能判断是否被修改，但是该方案不支持公开审计。私有云可以完全解决不可信或半可信云存储系统问题，但是仍然需要考虑数据的完整性校验问题。

本文在算法的选择上采用经国家商用密码管理局认定的国产密码算法，国产密码算法已经在国内的银行、通信、医院等各大行业得到大规模应用，具备实际应用条件。在算法安全性上，目前国际上通用的杂凑密码算法 MD5、SHA-1、HAVAL 等已被我国密码学家王小云破解[11,12]。我国密码算法公开后，国内外众多行业专家对其进行了全面的安全测评，从目前公开的资料来看，我国密码算法的安全性整体优于美国的密码算法[13-15]。

2　方案设计

2.1　算法设计

数据加扰思想源自军事通信中的信号加扰处理，用于防止非授权者的窃听活动。在密码学中数据加扰可以有效隐藏明文数据的统计特性，提升其抗扩散能力。DLSHE 算法是基于国产密码算法 SM2、SM3 和 SM4[16~18]共同构成的一种数据线性加扰混合加密算法，本算法的重点在于加密细粒度、线性分割线、数据加扰控制、完整性验证和双密钥管理上。加密细粒度指对明文数据第一次进行最小化分块；线性分割线指对加密细粒度进行数据比例划分，处于分界线之前的数据使用 SM4 算法加密，处于分界线之后数据用 SM2 算法加密，最终在加密细粒度和线性分割线的共同作用下形成子明文数据块；数据加扰指对形成的子明文数据块分别进行按行读取，然后在每一行数据的末尾添加当前时间函数毫秒值的后三位，最终形成具有真随机性的加扰明文数据；数据的完整性验证主要包括报文摘要算法和数字签名算法，用于防止数据非法窜改和用户行为抵赖问题；双密钥管理指利用保护密钥加密工作密钥，工作密钥以密文的形式存储在云端，用户只需存储保护密钥。DLSHE 算法流程如图 1 所示。

DLSHE 算法详细加密过程如下：

a)读取需要加密的明文数据 M；

b)将明文数据 M 按照分割策略进行数据分割，数据分割完成后形成 $M_1,M_2,M_3,M_4,M_5,\ldots$ 等子明文数据。分割策略由加密细粒度和线性分割线共同决定，在实际应用中用户可以根据需求动态设置加密细粒度和线性分割线。

c)系统分别读取子数据 $M_1,M_2,M_3,M_4,M_5,\ldots$，对每个子数据块进行数据加扰处理，最终形成子加扰数据 $M_{11},M_{22},M_{33},M_{44},M_{55},\ldots$。

d)系统对 $M_{11},M_{22},M_{33},M_{44},M_{55},\ldots$ 进行加密处理，处理方式为交替使用 SM4 和 SM2 算法对子加扰数据进行加密，最终形成子密文数据 $C_1,C_2,C_3,C_4,C_5,\ldots$。

e)为防止数据非法窜改和用户行为抵赖问题，利用 SM3 算法对明文数据 M 产生报文摘要，然后使用 SM2 算法的私钥进行数字签名，签名数据经过加扰后使用 SM2 算法的公钥进行加密，最终形成密文数据 C_{n+1}。

f)将密文数据 $C_1,C_2,C_3,C_4,C_5,\ldots,C_{n+1}$ 进行合并形成最终密文 C。

g)利用 SM2 的公钥加密 SM4 的私钥（工作密钥）形成密钥密文存储在云端，用户本地只存储 SM2 的私钥（保护密钥）。

DLSHE 算法详细解密过程如下：

a)利用 SM2 的私钥解密密钥密文，得到 SM4 的私钥。

b)将密文数据 C 按照定义规则拆分成子密文数据 $C_1,C_2,C_3,C_4,C_5,\ldots$ 和 C_{n+1}。

c)将子密文数据 $C_1,C_2,C_3,C_4,C_5,\ldots$ 按照解密策略，交替使用 SM4 和 SM2 算法进行解密，形成 $M_{11},M_{22},M_{33},M_{44},M_{55},\ldots$ 子加扰数据。

d)分别对 $M_{11},M_{22},M_{33},M_{44},M_{55},\ldots$ 进行数据去扰处理，得到 $M_1,M_2,M_3,M_4,M_5,\ldots$ 子明文数据。

e)合并 $M_1,M_2,M_3,M_4,M_5,\ldots$ 所有子明文数据，得到原始数据 M。

f)将密文数据 C_{n+1} 使用 SM2 算法进行解密，产生加扰数字签名，然后进行数据去扰产生数字签名，对签名进行验证并产生原始报文摘要。

g)对解密后的明文数据 M 进行二次摘要产生新的报文摘要，对比分析两次报文摘要的值，如果相等即数据未窜改，如果不等即数据被窜改或签名有问题。

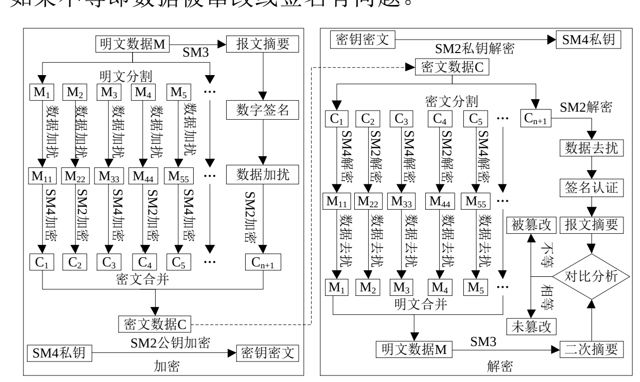


图 1　DLSHE 算法流程图

Fig. 1　DLSHE algorithm flow chart

2.2　算法安全性分析

2.2.1 密钥安全性分析

现代密码学的基本设计准则为算法公开，安全性完全取决于对密钥的保密。DLSHE 算法在密钥的管理上采用了双密钥管理机制，有效的增强了密钥的安全存储方式。基本原理为：DLSHE 算法的密钥由工作密钥和保护密钥两部分组成，工作密钥由 SM4 的私钥和 SM2 的公钥共同构成用于加解密数据，工作密钥只需要加密 SM4 私钥部分，最终以密文的形式存储在云端；保护密钥由 SM2 的私钥构成存储于客户端本地，任何用户如果想解密密文数据，必须使用保密密钥解密工作密钥，意味着用户必须同时使用两把密钥才能解密数据。

ChinaXiv合作期刊

虽然双密钥管理机制确保了工作密钥的安全性，但是用户仍然需要安全存储保护密钥，为此 DLSHE 算法增加了多因素安全依赖参数，形成不完全依赖密钥保护的安全机制，详细内容见 2.2.3 抗攻击性分析内容。

2.2.2 抗扩散性分析

在密码学中扩散性指的是明文数据的每一位发生改变都会导致密文数据的诸多位发生改变，通过这种方式可以隐蔽明文数据的统计特性。本文选取同一明文数据和密钥用于实验测试，并选取三种算法进行对比分析，实验中一次只改变一位明文数据，并统计密文位数的变化情况，共进行 6 组实验测试，抗扩散性测试结果如图 2 所示。

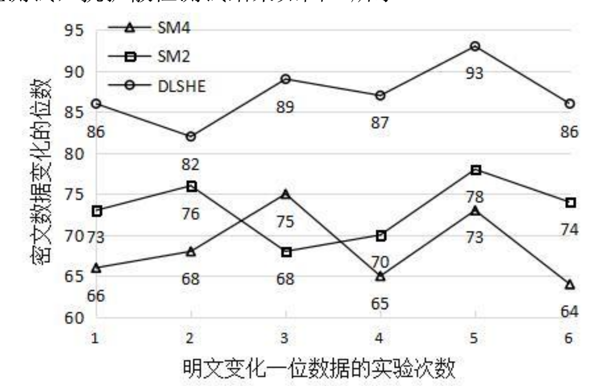


图 2　抗扩散性测试

Fig. 2　Anti-diffusion test

由图 2 可知，在只改变一位明文数据的情况下，分别统计出三种算法密文变化位数的均值，其中 SM4 算法密文变化位数的均值约为 68 位，SM2 算法密文变化位数的均值约为 73 位，DLSHE 算法密文变化位数的均值约为 87 位。由于 DLSHE 算法添加了加扰数据，相当于有多位的明文数据发生变化，因此在抗扩散性测试中密文变化的位数最多。通过实验分析对比，可得出 DLSHE 算法的抗扩散能力最强，更加有效的隐蔽了明文数据的统计特性。

2.2.3 抗攻击性分析

实际上 DLSHE 算法的抗攻击能力并不完全依赖于密码算法和密钥，还取决于数据加扰方式、加密细粒度和线性分割线，详细内容如表 1 所示，其中 A_1 表示算法安全性；A_2 表示密钥安全性；A_3 表示数据加扰方式；A_4 表示加密细粒度；A_5 表示线性分割线；Y 表示依赖，N 表示不依赖，同时与 SM4 和 SM2 算法进行对比分析。假如攻击者获取部分明文数据和密文数据，但是明文数据在数据加扰后才进行加密生成密文，实际明文数据和密文数据的对应关系已经被破坏掉，同时数据加密细粒度和线性分割线采用用户自定义模式，攻击者很难对加密信息进行解密。甚至用户密钥在被盗的情况下，攻击者还必须同时知道加密过程中使用的算法、加密细粒度、线性分割线和数据加扰方式这些条件，才可能获取原始明文数据。通过以上分析可知，DLSHE 算法的安全性不再完全依赖单一的密钥保护和算法安全性，它还取决于数据加扰方式、加密细粒度和线性分割线等多因素安全参数，这种方式有效的提升了算法自身的抗攻击能力，能够为企业私有云环境下的数据提供安全保证。

表 1　安全参数依赖性分析

Table 1　Security parameter dependency analysis

算法名称	A_1	A_2	A_3	A_4	A_5
SM4	Y	Y	N	N	N
SM2	Y	Y	N	N	N
DLSHE	Y	Y	Y	Y	Y

3　实验结果及分析

实验平台：利用 Hadoop 搭建企业私有云数据存储环境，由 6 台计算机组成，基本配置为 CPU i3-2120 主频 3.3 GHz，4 GB 内存，1 TB 硬盘，选择 CentOS 6.5 版本作为每台服务器的操作系统；开发了基于 LAMP 的一个云存储加密系统，模拟企业私有云环境下的数据操作流程。

3.1　云存储加密系统

云存储加密系统能够满足企业用户对云文件的基本操作要求，包括文件的上传、下载、修改、删除和共享功能。精细化的权限控制，公共区域文件用户仅拥有查看和下载权限，只有系统管理员输入相应密钥方可获取文件的全部操作权限。

企业用户登录个人云空间，方可拥有自己文件的全部操作权限，此时可以使用 DLSHE 算法模块对核心重要数据进行加解密操作。本文着重介绍云存储加密系统的 DLSHE 加解密模块，该模块具有密钥产生、报文摘要、数据签名、DLSHE 加解密等功能，详细内容如图 3 所示。

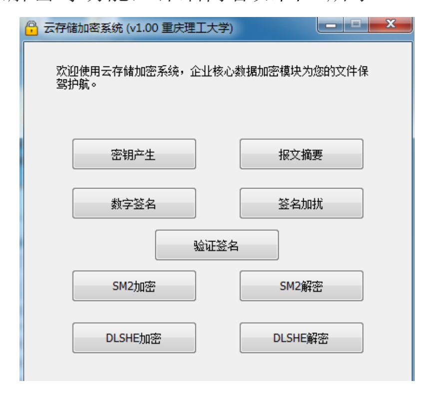


图 3　DLSHE 加解密模块

Fig. 3　DLSHE encryption and decryption module

3.2　DLSHE 算法的实现

a)DLSHE 算法的正确性测试，本文选取两行明文数据作为实验测试数据，数据加密细粒度以此测试数据为最小单元，线性分割比例选取 9：1 进行，SM4 加密算法是在 CBC 模式下，初始向量为 EE0CAD6B0059D77EE3D4F0F16CA087E35，详细实验结果如表 2 所示。

从表 2 实验结果可知，明文数据经过 DLSHE 算法加密处理后，形成相应的密文数据，通过对密文数据的拆分、去扰、解密等操作，获取相应的明文数据、报文摘要和数字签名。通过对比分析发现与原始的明文数据、报文摘要和数字签名完全相同，证明 DLSHE 算法是满足数据加解密要求的，可以在企业私有云环境下应用。

b)DLSHE 算法加密文件类型测试，实验中选取了 txt、doc、png、zip 等多种文件类型用于加解密测试（详细文件加密类型如表 3 所示），均可达到预期加解密效果。实际上 DLSHE 算法采用的是基于文件 IO 流的数据加解密方式，所以可以支持任意格式的文件类型，从而进一步扩展了其应用范围。

为展现文件加密效果，选取一个 0.23MB 大小的 txt 文件用于加密测试，系统启动 DLSHE 加解密模块，具体操作界面如图 3 所示。具体操作流程如下：

(a)用户点击密钥产生模块，系统将分别创建 SM4 私钥文件、SM2 公钥文件和 SM2 私钥文件；

(b)用户点击报文摘要模块，选择明文数据，产生报文摘要文件；

chinaXiv:201901.00027v1

(c)用户点击签名模块，选择相应的报文摘要进行签名；

(d)用户点击签名加扰模块，对签名进行数据加扰；

(e)用户点击 SM2 加密模块，选择加扰签名进行加密，产生相应密文文件；

(f)用户点击 DLSHE 加密模块，系统读取 SM4 私钥和 SM2 公钥文件，开始对文件进行线性加扰混合加密并合并所有密文，加密完成后打开原始 txt 文件如图 4 所示。

表 2　DLSHE 算法实验结果

Table 2　DLSHE algorithm experiment results

明文数据	ABCD2354GTR689DFOKM6E6 H7HG6809YGFD56HGG76980
SM4 私钥	ACC994D41FA7FC1D7D35B6EAFD69E80A
SM2 公钥	04134EA21FCAE5D68E058FDC1A9291F6152D62C02DE 4EECAFEAC61B976D38F7AB6B413F3E9272267789542 835A1F1E59F6F07F81F063142CA1EB1F19F7E71CF7A1
报文摘要	E631A148483E0BD91C839ED6558B84C9BF641EA69FE C059AF707855296B979B6
数字签名	304402204E98DFEFC7451FE7B4995199F02E72B218E57 6D53732C8D3C058B142281ED34A02205A4D8B3810FB B23C617198F0209A28719890E7509222BE346930A569D 62AE6E9
密文数据	BB37F31C19E671EDCA443C4A9947490C0A988DFD163 A751C9B32A94A4FFE7ADE54F8E09A8B073122A879E EA33D4921AA04697EDAE8C0C1D2F864CFADAC00B1 A8B1A86771CA931FF00E24DE1C14B313FF4FD6F4124 DC4B20CFADBADEDC9C9DD837610A620393FA01B3B 9F00C20C709301DEFB2544F403D4A6A9757CD84AF23 E7FA26165A3E6748D818FD92A5E032D1125022259329 358308191022100F33BD3CA205CFC3C198D00891A55F 86D6F451C42E23B51E86CB0D713D54D682F022069690 E4C86088E4A56773BEF5C224F6C64F6EC420C58B7AC 98FC36F4B76830F70420E8CD3D5F92B38AEF6A5FD35 F13E7074974300A0B3E21D169D6FE9BB44CB5D8F704 2842412B945B2AB5B68FF0410269207832556A1CEBFA 4915790E9E165A4
SM2 私钥	4EC8F9C7B8E231535EACEA64200C211F8D6F732E6F6 F6CF4C89901B42EEED413
签名验证	304402204E98DFEFC7451FE7B4995199F02E72B218E57 6D53732C8D3C058B142281ED34A02205A4D8B3810FB B23C617198F0209A28719890E7509222BE346930A569D 62AE6E9
解密的报文摘要	E631A148483E0BD91C839ED6558B84C9BF641EA69FE C059AF707855296B979B6
解密的明文数据	ABCD2354GTR689DFOKM6E6 H7HG6809YGFD56HGG76980

表 3　文件加密类型测试

Table 3　File encryption type test

文件类型	文件大小	文件类型	文件大小
txt	0.23 MB	wma	74.6MB
doc	1.24 MB	mp4	36.2MB
png	1.13 MB	jpg	0.83MB
avi	68 MB	rmvb	62.4MB
zip	126.4 MB	gif	1.62MB

c)DLSHE 算法加解密效率测试，本文选取 1.36GB 大小的压缩包文件用于实验测试，文件内容格式包括 txt、pdf、doc、avi 等 6 种文件类型。加密细粒度的选择为 2056 比特，线性分割比例为 9：1。默认情况下 Hadoop 的数据分块大小为 64MB，为充分测试加密算法在云平台下的加解密效率，分别选取了 2MB、4MB、8MB、16MB、32MB、64MB 大小的数据分块。实验中选取了 DLSHE 算法、SM4 算法和 SM2 算法用于对比测试，每种算法分别进行了 6 组的加密实验和 6 组的解密实验，并求其计算时间的平均值，加解密测试结果如图 5 和 6 所示。

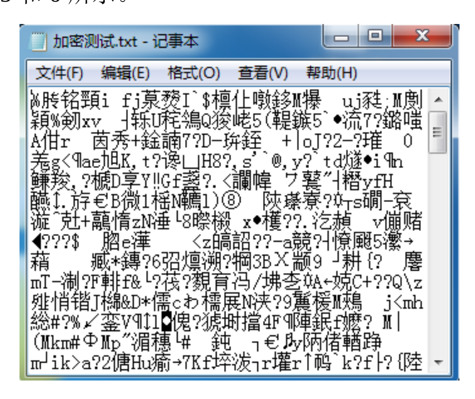


图 4 文件加密效果

Fig. 4　File encryption effect

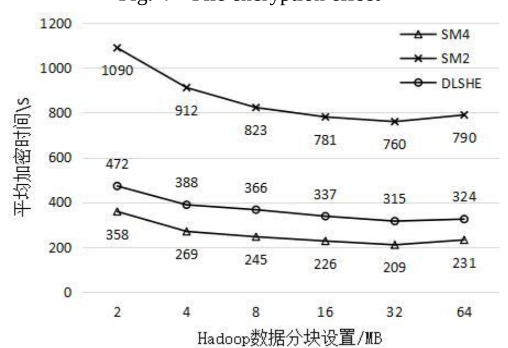


图 5　DLSHE 加密效率测试

Fig. 5　DLSHE encryption efficiency test

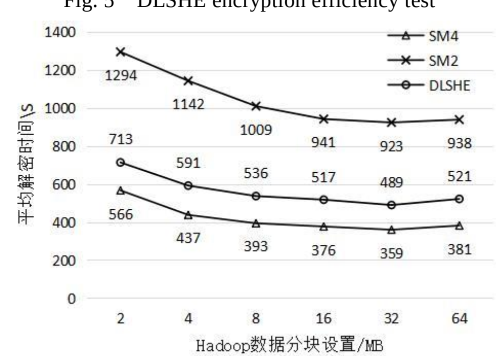


图 6　DLSHE 解密效率测试

Fig. 6　DLSHE decryption efficiency test

由图 5 和 6 分析对比可知，Hadoop 的数据分块大小对数据的加解密效率存在着一定的影响，当数据分块在 16 MB、32 MB 和 64 MB 时加解密效率最高趋于稳定状态，但是当数据分块过小时，例如 2 MB 的数据分块导致数据的加解密时间陡增，其主要原因包括：计算机需要频繁调用加解密算法处理数据，消耗计算资源;分布式计算条件下需要对分块的结果进行整合排序，当分块过小时势必要消耗更多的时间。所以企业在搭建私有云平台时，需要考虑合理的划分数据块大小，避免计算资源的浪费。

对比分析三种加密算法的平均加解密时间消耗可知，SM2 算法的平均加解密时间消耗最大，SM4 算法的平均加解密时间消耗最小，DLSHE 算法的平均加解密时间消耗略上高于 SM4 算法，但是用户可以通过线性分割线的设置来进一步降低加解密时间。同时由于本文只使用了 6 台普通个人计算机搭建了一个小的云计算服务器集群，如果是在大规模的计

chinaXiv:201901.00027v1

ChinaXiv合作期刊

算集群下，这种时间上的差距会更小。

d)DLSHE 算法安全性测试，本算法的安全性由两部分构成，一部分是由 SM4 和 SM2 算法的安全性共同决定的，另一部分是由不公开的加密策略决定的。

算法安全性对比：SM4 算法在抗差分攻击方面目前最好的结果为 23 轮[19]；在抗线性攻击方面目前最好的结果为 23 轮[20]；在多维线性攻击方面目前最好的结果为 23 轮[20]；在矩形攻击方面目前最好的结果为 18 轮[21]；在积分攻击方面目前最好的结果为 14 轮[22]，整体来说目前没有任何一种攻击手段能够对其进行全轮攻击。SM2 算法的设计是基于广义 ELGamal 算法，但是该算法安全性不高，在选择明文攻击、选择密文攻击和自主选择密文攻击的多种攻击模式下，很容易遭受到 IND-CAA2（不可区分性自主选择密文攻击），为此使用 Hash 函数来增强其安全性，使安全级别达到 IND-CAA2 标准[23]；在数字签名时最强的攻击行为是自主选择消息攻击，为此采用了 EUF-CMA（自主选择消息攻击下存在不可伪造）标准来应对；在密钥替换攻击方面，采用了将签名者 ID、公钥和消息源一起 Hash 的防御手段[24]，整体来说该算法的安全性优于 SM4 加密算法，但是其算法计算复杂度大消耗时间长。DLSHE 算法具备上述两种算法的所有抗攻击能力，但是其安全性却优于上述两种算法中的任何一种，首先在密钥的管理上采取了双密钥管理机制，增强了密钥的安全存储方式，其次在抗扩散性实验中其抗扩散能力最强（详细内容见 2.2.2 抗扩散性分析），主要原因是采用了数据加扰的防御方式，最后由于 DLSHE 算法的加密策略对外是不公开的，攻击者猜测不出加密策略中的加密粒度大小、线性分割线位置和数据加扰方式，从而进一步增强了算法的安全性。

在云存储加密系统中，加密细粒度和线性分割线可根据用户需求改变，数据加扰方式采用的是当前时间函数，从安全的角度来说加密策略具有随机性，攻击者很难统计出加密策略的规律。同时由于加密策略的随机性，导致 DLSHE 算法的安全性并不是一层不变的，在实验测试中将算法的安全等级按照 0 到 1 之间划分，在数据加扰方式一样的条件下，分别进行了 6 组实验测试，其中 SM4 或 SM2 算法在 6 组实验测试中安全等级不会因加密策略的变化而变化，在第 2 组、第 4 组和第 6 组实验测试中，由于加密细粒度设置较大且线性分割线的比例设置简单，攻击者可能猜测出加密策略的概率就大，故 DLSHE 算法的安全等级有所下降；在第 1 组、第 3 组和第 5 组实验测试中，加密细粒度设置较小且线性分割线的比例设置复杂，攻击者可能猜测出加密策略的概率就小，故 DLSHE 算法的安全等级有所提升，在理想情况下是无限趋近于最高安全等级 1 的，详细内容如图 7 所示。

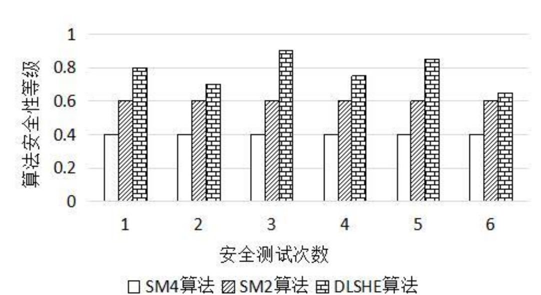


图 7 DLSHE 安全性对比测试

Fig. 7 DLSHE safety comparison test

f)本文对 DLSHE 算法的密钥安全性、抗扩散性和抗攻击性方面进行了全面分析，并通过实验测试了算法的正确性、加密支持的文件类型、加解密效率和安全性，综合考虑所有影响因素，最终确定了 DLSHE 算法，该算法是一种在安全性和效率上同时兼顾的线性加扰混合加密算法，能够为私有云环境下的企业核心数据提供更好的安全保障，具有较大的应用价值。

4 结束语

企业私有云环境下的数据安全问题，主要包括数据的安全存储和完整性校验。针对以上问题，本文提出利用数据线性加扰混合加密思想，增强算法安全依赖参数，解决单一密钥保护问题；利用双密钥管理机制，增强密钥的安全存储方式；利用报文摘要算法和数字签名算法，解决数据防窜改和用户行为为抵赖问题。最后通过实验对 DLSHE 算法进行了全面测试，可达到企业私有云环境下的数据安全保护要求，且相对于传统加密算法在安全性方面有大幅度提升。

参考文献：

[1] 冯登国，张敏，张妍，等. 云计算安全研究 [J].软件学报,2011, 22(1): 71-83. (Feng Dengguo, Zhang Min, Zhuang Yan, *et al.* Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83.)

[2] 闫乐乐，李辉. 基于复合混沌序列的动态密钥 AES 加密算法 [J]. 计算机科学, 2017, 44(6): 133-138,160. (Yan Lele, Li Hui. Dynamic key AES encryption algorithm based on compound chaotic sequence [J]. Computer Science, 2017, 44(6): 133-138+160.)

[3] 张祎江. 基于 3DES-ECC 算法的网络信息加密研究[J].科技通报, 2014, 30(4): 229-231+235. (Zhang Yijiang. Study on network information based on 3DES-ECC encryption algorithm[J]. Science and Technology Bulletin, 2014, 30(4): 229-231,235.)

[4] 周文婷，朱娇娇. DES 加密算法的一种改进方法[J]. 计算机安全, 2012, 18(9): 47-50.(Zhou Wenting, Zhu Jiaojiao. An improvement method to implement the DES encryption algorithm [J]. Computer Security, 2012, 18 (9): 47-50.)

[5] 肖振久，胡驰，蒋正涛，等. AES 与 RSA 算法优化及其混合加密体质 [J]. 计算机应用研究, 2014, 31(4): 1189-1194,1198. (Xiao Zhenjiu, Hu Chi, Jiang Zhengtao, *et al.* Optimization of AES and RSA algorithm and its mixed encryption system [J]. Application Research of Computers, 2014, 31 (4): 1189-1194,1198.)

[6] 王奎，李立新，余文涛，等. 基于 ECC 算法的 TLS 协议设计与优化 [J]. 计算机应用研究. 2014, 31(11): 3486-3489. (Wang Kui, Li Lixin, Yu Wentao, *et al.* Design and optimization of TLS protocol based on ECC[J]. Application Research of Computers. 2014,31(11): 3486-3489.)

[7] 冯朝圣，秦志光，袁丁.云数据安全存储技术 [J]. 计算机学报, 2015, 38(1): 150-163. (Feng Chaosheng, Qin Zhiguang, Yuan Ding. Techniques of secure storage for cloud data [J]. Chinese Journal of Computers, 2015, 38(1): 150-163.)

[8] Erway C, Kupcu A, Papamanthou C, *et al.* Dynamic provable data possession [C]//Proc of ACM Conference on Computer and Communications Security. NewYork: ACM Press, 2009: 213-222.

[9] Wang Cong, Wang Qian, Ren Kui, *et al.* Towards secure and dependable storage services in cloud computing [J]. IEEE Trans on Service Computing, 2012, 5(2): 220-232.

[10] 徐剑，周福才，陈旭，等. 云计算中基于认证数据结构的数据外包认证模型 [J]. 通信学报, 2011, 32(7): 153-160. (Xu Jian, Zhou Fucai, Chen Xu, *et al.* Data outsourcing authentication model based on authenticated data structures for cloud computing [J]. Journal of

chinaXiv:201901.00027v1

ChinaXiv合作期刊

Communications, 2011, 32 (7): 153-160.)

[11] Bai D, Yu H, Wang G, *et al*. Improved boomerang attacks on round-reduced SM3 and keyed permutation of BLAKE256 [J]. IET Information Security, 2015, 9(3): 167-178.

[12] Wang X, Feng D, Lai X, *et al*. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD [EB/OL].(2004-07-17) [2018-08-10]. https://eprint. iacr. org/2004/199. pdf.

[13] Zhao Shijun, Xi Li, Zhang Qianying, *et al*. Security analysis of SM2 key exchange protocol in TPM-2. 0 [J]. Security & Communication Networks, 2015, 8(3): 383-395.

[14] Christina B, Naya-Plasencia M, Suder V. Scrutinizing and improving impossible different attacks: Applications to CLEFIA, Camellia, LBlock and Simon [C]//Proc of International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2014: 179-199.

[15] Todo Y. Integral cryptanalysis on full MISTY1 [C]//Advances in Cryptology. Berlin: Springer, 2015: 413-432.

[16] 汪朝辉，张振峰. SM2 椭圆曲线公钥密码算法综述 [J]. 信息安全研究, 2016, 2(11): 972-982. (Wang Zhaohui, Zhang Zhenfeng. Overview on public key cryptographic algorithm SM2 based on elliptic curves [J]. Journal of Information Security Research, 2016, 2(11): 972-982.)

[17] 王小云，于红波. SM3 密码杂凑算法 [J]. 信息安全研究, 2016, 2(11): 983-994. (Wang Xiaoyun, Yu Hongbo. SM3 cryptographic hash algorithm [J]. Journal of Information Security Research, 2016, 2(11): 983-994.)

[18] 吕述望，苏波展，王鹏，等. SM4 分组密码算法综述 [J]. 信息安全研究, 2016, 2(11): 995-1007. (Lyu Shuwang, Su Bozhan, Wang Peng, *et al*. Overview on SM4 algorithm [J]. Journal of Information Security Research, 2016, 2, (11): 995-1007.)

[19] Su Bozhan, Wu Wenling, Feng Dengguo, *et al.* Security of the SM4 block cipher against differential cryptanalysis [J]. Journal of Computer Science and Technology, 2001, 26(1): 130-138.

[20] Liu Mingjie, Chen Jiazhe. Improved linear attacks on the chinese block cipher standard [J]. Journal of Computer Science and Technology, 2014, 29(6): 1123-1133.

[21] 薛萍. 对分组密码算法 SM4 的矩形攻击 [D]. 济南：山东大学, 2012. (Xue Ping. Rectangle attack of reduced SMS4 block cipher [D]. Jinan: Shandong University, 2012.)

[22] 钟名富，胡予濮，陈杰. 分组密码算法 SM4 的 14 轮 Square 攻击 [J]. 西安电子科技大学学报：自然科学版, 2008, 35(1): 105-109. (Zhong Mingfu, Hu Yupu, Chen Jie. Square attack on the 14-round block cipher SMS4. Journal of XiDian University: Natural Science, 2008, 35(1): 105-109.)

[23] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[C]// Proc of International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1998: 13-25.

[24] Zhang Zhenfeng, Yang Kang, Zhang Jiang, *et al.* Security of the SM2 signature scheme against generalized key substitution attacks [C]// Proc of International Conference on Research in Security Standardisation. Berlin: Springer, 2015: 140-153.

chinaXiv:201901.00027v1